Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): RECOP017

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on April 24, 2006

Signature: Veronica Pula

Typed or printed name: Veronica Pula

Application Number	Filed
09/654,347	August 30, 2000

First Named Inventor: Douglas B. Moran

Art Unit	Examiner
2136	Ronald Baum

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 55,285
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

Clover Huang
Signature

Clover Huang
Typed or printed name

408-973-2594
Telephone number

4-24-2006
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Douglas B. Moran	Examiner:	Ronald Baum
Application No.:	09/654,347	Art Unit:	2136
Filed:	August 30, 2000	Docket No.:	RECOP017
Title:	SYSTEM AND METHOD FOR USING TIMESTAMPS TO DETECT ATTACKS		

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in a prepaid envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

April 24, 2006

Veronica Pula

REMARKS IN SUPPORT OF PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This is in response to the Office Action mailed January 24, 2006. The following remarks are respectfully submitted in support of Applicants' pre-appeal brief request for review filed herewith.

Claims 1-12, 16, and 17 are pending. Claims 1, 16, and 17 are independent. Claims 2-12 depend from claim 1. The Examiner has rejected claims 1-12, 16, and 17 under 35 U.S.C. 103(a) as being unpatentable over Porras in view of Beardsley. Applicants respectfully submit that the cited references do not establish a prima facie case of obviousness, such that the Examiner clearly erred in rejecting the claims as obvious.

Neither Porras nor Beardsley, either singly or in combination, describes an analysis engine configured to "identify a backward time step" in a logfile, "determine that the backward time step is associated with an event," and "assign a suspicion value to the event based at least in part on the backward time step," as recited in claim 1.

Porras teaches consolidating alerts that are indicative of a common incident. The January 24, 2006 Office Action, at page 7-8, acknowledges that Porras does not disclose "identify a backward time step in the logfile by identifying a first entry for which an associated first log entry time is earlier in time than a second log entry time associated with a second log entry entered in the logfile prior to the first entry" and asserts that Beardsley teaches "using time stamps to correlate data processing event times in connected data processing units" and that "the Beardsley et al invention also clearly encompasses the logging of detected intrusions on a host system," and that "it would have been obvious... to have been motivated to combine the Porras et al system... with the Bearsley et al teachings."

Beardsley describes a way to determine an event time on a host clock when the event is logged on a peripheral system clock. In Beardsley, the event has already been detected. A time difference between a host and a peripheral system is used to convert the peripheral time to a host time, i.e., when host times are not synchronized, the difference between the host time stamp and the peripheral time stamp is added to the peripheral time stamp to determine the event time on the host clock. Beardsley, column 2, line 47 to column 3, line 4. By contrast, claim 1 recites identifying a backward time step, determining that the backward time step is associated with an event, and assigning a suspicion value to the event. The backward time step is identified and is determined to be associated with an event. For example, the backward time step may reflect an attempt by an intruder to camouflage an unauthorized action taken by the intruder by altering the system clock, as described in the application at page 83, line 13 to page 85, line 13. Beardsley only describes a difference in time between a host and a peripheral system, e.g., due to a lack of clock synchronization between the host and the peripheral system, and not a backward time step in a logfile as recited in claim 1. The difference in time described by Beardsley is not associated with an event, and is merely used to convert the peripheral time to a host time.

Neither Porras nor Beardsley describes a backward time step as recited in claim 1. Therefore, the obviousness rejection of claim 1 is not prima facie. As such, claim 1 is believed to be allowable.

Claims 2-12 depend from claim 1 and are believed to be allowable for the same reasons described above.

Claim 16 recites a method executed by the system of claim 1. Therefore, it is believed that claim 16 is also allowable.

Claim 17 recites program code for carrying out the method of claim 16. Therefore, it is believed that claim 17 is also allowable.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks.

Respectfully submitted,

Dated: 4-24-2006

Clover Huang

Clover Huang
Registration No. 55,285
V 408-973-2594
F 408-973-2595

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014